In the Claims

1. (currently amended) A system for encrypting data files, comprising:

a computer;

a storage device connected to said computer;

an application loaded on said computer for storing and retrieving data files on said storage device; ~~and~~

a program executing on said computer, independently of said application, for intercepting said data files to be stored by the application on said storage device to encrypt them before they are stored.

said program includes an encrypt key for encrypting and decrypting data files and an application identifier for specifying which application to launch; and

wherein said encrypt key and application identifier are stored together in an encrypted file.

2. (original) The system of claim 1, wherein said program intercepts data files to be retrieved by said application from said storage device to decrypt them.

3. (original) The system of claim 2, wherein said program decrypts said data files retrieved by said application in memory.

4. The system of claim 3, wherein said program does not store unencrypted versions of the encrypted data files on said storage device.

5. (original) The system of claim 1, wherein said program encrypts said data files automatically without user intervention.

6. (original) The system of claim 1, wherein said program decrypts said data files automatically without user intervention.

7. (cancelled)

8. (cancelled)

9. (original) The system of claim 8, wherein said encrypted file is encrypted with a passkey selected from a group of passkeys.

10. (original) The system of claim 8, wherein said encrypted file is encrypted with a passkey generated from a feature of the encrypted file.

11. (original) The system of claim 10, wherein said feature is a size of the encrypted file.

12. (original) The system of claim 10, wherein said feature is a time the encrypted file is created.

13. (original) The system of claim 10, wherein said feature is a date the encrypted file is created.

14. (original) The system of claim 8, wherein said encrypted file is encrypted with a passkey having more than one component.

15. (original) The system of claim 9, wherein said program decrypts said encrypted file with said passkey.

16. (original) The system of claim 1, wherein said program causes said application to execute on said computer.

17. (original) The system of claim 7, wherein said program decrypts said data files with said encrypt key.

a' mnt

18. (currently amended) A system for copying data files, comprising:

a computer;

a first storage device connected to said computer;

an application loaded on said computer for storing and retrieving data files on said first storage device;

a second storage device accessible by said computer; and

a program executing on said computer, independently of said application, for copying to said second storage device said data files stored by said application on said first storage device.

wherein said second storage device is located remotely from said first storage device.

19. (cancelled)

20. (original) The system of claim 18, wherein said copying is for the purposes of backing up said data files.

21. (original) The system of claim 18, wherein said copying is for the purposes of replicating said data files.

22. (original) The system of claim 18, wherein said program intercepts said data files to be copied to said second storage device and encrypts them before they are copied.

23. (original) The system of claim 22, wherein said program intercepts said data files to be retrieved by said application from said second storage device to decrypt them.

24. (original) The system of claim 23, wherein said program decrypts said data files retrieved by said application in memory.

25. (currently amended) A method for encrypting data files comprising the steps of:

commanding an application to store a data file on a storage device connected to a computer;

intercepting said data file from the application before said data file is stored on said storage device;

determining whether said data file is to be encrypted;

encrypting said data file; ~~and~~

storing said data file on said storage device; and

decrypting said data file in memory.

26. (original) The method of claim 25, further comprising the additional step of encrypting said data file automatically without user intervention.

27. (currently amended) The method of claim 25, further comprising the additional step of intercepting said data file to be retrieved from ~~said~~ a second storage device.

28. (cancelled)

29. (original) A method for encrypting a file comprising the steps of:

generating a file based on specified parameters;

varying a size of the file;

selecting a passkey component from a list of possible passkey components;

combining the file size and the passkey component to form a passkey; and

using the passkey to encrypt the file.

30. (original) The method of claim 29, further comprising the additional step of noting a date the file was generated.

31. (original) The method of claim 29, further comprising the additional step of noting a time the file was generated.

32. (currently amended) A method for copying data files comprising the steps of:

storing a data file on a first storage device connected to a computer;

copying said data file on a second storage device accessible to said computer;

intercepting said data file from the application before said data file is stored on said second storage device;

determining whether said data file is to be encrypted;

encrypting said data file; and

storing said data file on said second storage device;

wherein said second storage device is located remotely from said first storage device.

33. (original) The method of claim 32, further comprising the additional step of copying said data file for the purposes of backing up said data file.

Q' cont

34. (original) The method of claim 32, further comprising the additional step of copying said data file for the purposes of replicating said data file.